

[PayPal](#)

>> [すべての規約を表示](#)

カード処理製品のPayPalデータ保護に関する付帯条項



最終更新日: 2021年12月1日

カード処理製品に関するPayPalデータ保護の付帯条項(「本付帯条項」)は、PayPalグループ法人(「PayPal」)が、カード決済、ゲートウェイサービス、または不正対策サービス(「決済サービス」)を売り手であるお客様(「売り手」または「お客様」)に提供する際、すべての製品、サービス、またはその他の提供品に適用されます。本付帯条項は、PayPalで支払うやPayPalのPay LaterサービスなどのPayPalウォレットサービスには適用されません。本付帯条項は、PayPalによるお客様への支払いサービスの提供を規定する、売り手とPayPalとの間の関連規約(「本規約」)の一部を構成するものとし、本付帯条項の条件と本規約の条件との間に矛盾がある場合、本付帯条項の条件を優先するものとし、本付帯条項で使用されているが定義されていない大文字の用語は、本規約で定められた意味を有するものとし、

本付帯条項は、(i)規約に記載されている発効日、または(ii)本付帯条項に関連してお客様に掲示または提供される通知に記載されている発効日のいずれか遅い日付をもって発効します。弊社は、いつでも本付帯条項を改定することができます。改定版は、特に指定がない限り、PayPalのウェブサイトに掲載した時点で有効となります。変更によりお客様の権利を縮小したり、責任を増大したりする形で本付帯条項を変更した場合、本規約で定められた期間内に、弊社ウェブサイトの[ポリシーの更新]ページに通知を掲載します。お客様が本付帯条項の変更に同意しない場合、お客様は、支払いサービスの使用をいつでも中止することができます。

定義

次の用語は、本付帯条項で使用される場合、以下を意味します。

「**管理者**」とは、*個人データの取扱いの目的および手段を決定する法人を意味します。または、当該用語(または同様の機能に対応する用語)がデータ保護法に規定されている場合には、「管理者」は、適用可能なデータ保護法に規定される意味を有するものとし*ます。

「**顧客**」とは、支払いサービスを使用し、本付帯条項の目的上のデータ対象者である、お客様の顧客を意味します。

「**顧客データ**」とは、(i)顧客が売り手に提供し、支払いサービスの売り手による使用を通じて売り手がPayPalに渡す個人データ(ii)支払いサービスの売り手による使用を通じてPayPalが顧客の端末およびブラウザから収集し得る個人データを意味します。

「**データ保護法**」とは、支払いサービスの提供に適用される、適用可能なデータ保護に関する法律、規制、指令、規制要件、および実施規範を意味し、これらに対する修正と関連する規制や文書を含みます。例えば、カリフォルニア州消費者プライバシー法(2018, Cal.Civ.Code §1798.100 et seq)、EU一般データ保護規則2016/679(GDPR)、1988年オーストラリア連邦プライバシー法、個人情報保護および電子文書法(カナダ)、個人情報(プライバシー)条例(Cap.486)(香港)、ブラジル一般データ保護法(2018年連邦法第13709号)、および2012年個人情報保護法(シンガポール)、などが挙げられます。

「**PayPalグループ法人**」とは、PayPal, Inc.およびPayPalまたはその後継者が随時、直接間接を問わず所有または管理するすべての会社を意味します。

「**個人データ**」とは、識別された自然人または識別可能な自然人(「データ対象者」)に関する情報を意味します。識別可能な自然人とは、直接的または間接的に、特に氏名、識別番号、位置情報、オンライン識別子などの識別子、または当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的なアイデンティティに固有の1つまたは複数の要素を参照して、識別することができる人物を指します。

「**取扱い**」または本付帯条項で使用される場合に同様の機能を指す用語は、適用可能なデータ保護法で規定された意味を有するものとし

管理者としてのPayPal

PayPalは、本付帯条項に基づく顧客データの取扱いに関して、管理者に適用されるデータ保護法の要件を遵守し(顧客データの取扱いに関連して常に適切なセキュリティ対策を実施および維持することを含みますが、これに限定されません)、データ保護法の売り手による違反につながる可能性の高い行為を顧客データに関して故意に行わず、また行うことを許可しないものとします。顧客データ。PayPalは、顧客データを、本付帯条項に記載されている条件と同等の保護性を有する顧客データの保護に関する条件を含む書面による契約書に署名した第三者、下位の取扱い者、またはPayPalグループのメンバーにのみ移転するものとします。

支払いサービスに関連した顧客データの取扱い

両当事者は、売り手およびPayPalが、支払いサービスに関連して取り扱われるすべての顧客データに関して、それぞれ独立した管理者であることを認め、これに同意するものとします。したがって、PayPalは、当該顧客データの取扱いの目的および手段を独立して決定し、当該顧客データに関して売り手との共同管理者ではありません。

両当事者は、以下の限定された目的のために、PayPalによる顧客データおよび支払い取引データの使用、複製ならびに取扱いが許可されていることを認め、これに同意するものとします。

- 売り手およびその顧客への(不正対策ツールを含む)支払いサービスの提供および改善のために合理的に必要な場合。
- 不正な支払い取引の監視、防止、検出と、売り手、PayPal、第三者への損害の発生防止。
- PayPalに適用される支払いデータの取扱いおよび保持に適用される法的または規制上の義務(適用されるマネーロンダリング防止および本人確認の義務を含む)への準拠。
- PayPalの製品およびサービスの分析、開発、および改善。
- データ分析およびデータ表の社内使用(ただし、これらに限定されない)。
- お客様の個人またはユーザーの顧客データが特定できない場合における、顧客データおよび支払い取引データの集計と開示(地域または業界別の平均の計算を含む)。
- 適用される法的要件の遵守と、法律に従って情報開示の要求に対応することによる法執行機関の支援。
- データ保護法に準拠する目的に限り、売り手に通知するその他の目的。

売り手から顧客への通知

売り手は、(i)本付帯条項に記載の通り、顧客データを取扱う目的においてPayPalが独立した管理者であることを、自身のプライバシーポリシーにおいて顧客に通知し、(ii)売り手のプライバシーステートメントにPayPal プライバシーステートメントのリンク(www.paypal.com)を掲載するよう、商取引上の合理的な努力を払うものとしします。

相互扶助

両当事者は、他方当事者がデータ保護法のもとで独立した管理者としての責任を適切に果たすことができるように合理的に必要な範囲で、相互に協力することに合意します。売り手がデータ保護法の下で顧客による個人情報の開示請求または権利行使を受けた場合、売り手がそのような顧客のアクセス要求に直接応えるものとするに、両当事者は同意します。また、売り手は、www.paypal.comのプライバシーステートメントに記載されている指示に従って、PayPalを使用した支払いサービスに関連してデータ主体の権利を行使できることを顧客に通知するものとしします。また、PayPalは、セキュリティインシデントに関連して、影響を受ける顧客に通知する必要があると独自の判断において決定を下し、PayPalがそのような連絡を行う上で、影響を受ける顧客への連絡先情報を保持していない場合、売り手は、商業的に合理的な努力を払って、データ保護法に基づきPayPalが影響を受けた顧客への通知義務を遵守するという限られた目的のために、売り手が有する顧客の情報をPayPalに提供するものとしします。

国境を越えたデータの移転

両当事者は、PayPalが、本規約に基づいて取り扱う顧客データを、支払いサービスを提供するために必要に応じて収集された国以外に移転する場合があることに同意するものとしします。PayPalが本付帯条項の下で保護された顧客データを、データが収集された国の関連規制当局が妥当性の判断を下していない管轄区域に同データを移転する場合、PayPalは、適用されるデータ保護法に従って、顧客データの移転に適切な保護措置が取られることを保証します。例えば、GDPRを遵守するため、顧客の個人データを他のPayPalグループの他のメンバーに移転する際は、管轄監督機関が承認した拘束力のある法人規則およびその他のデータ移転方法を使用します。

欧州連合、スイス、欧州経済領域、その加盟国または英国に拠点を置くお客様の顧客情報をPayPalへ移転することについて、お客様およびPayPalは、以下の事項に同意します。(i)お客様が本契約に署名することによって、データ輸出者であり管理者の役割を担う売り手として、適用可能な範囲において、GDPRに基づく個人データの第三国への移転のための標準契約条項に関する2021年6月4日の欧州委員会実施決定(EU)2021/914(「EUデータ移転条項」)に署名および受諾したとみな

され、データ輸出者として、当面の間、英国で施行されている2018年データ保護法第17C(b)条に基づいて国務大臣が策定した規制で指定される標準保護条項（「英国データ移転条項」）に署名および受諾したものとみなされること、(ii)該当する範囲において、PayPalによる本規約への署名は、データ輸入者であり管理者の役割を担う者として、PayPalがEUデータ移転条項に署名および受諾したものとみなされること、かつ、データ輸入者として、英国データ移転条項に署名および受諾したものとみなされること、ならびに(iii)両当事者は、EUデータ移転条項のモジュール1の規定に従うこと。欧州委員会または英国国務大臣(または該当する英国の権限を与えられた他組織)が、EUデータ移転条項または英国データ移転条項をそれぞれ改訂しその後公表した場合、または欧州委員会または英国国務大臣(または該当する英国の権限を与えられた他組織)が要求し施行した場合、両当事者は、改訂版のEUデータ移転条項または英国データ移転条項が現行のEUデータ移転条項もしくは英国データ移転条項に優先し、かつ、改訂版EUデータ移転条項または英国データ移転条項がある場合は、その締結のために必要な一切の措置を取ることに合意します。EUデータ移転条項(モジュール1)および英国データ移転条項は、参照により本規約に組み込まれ、以下の詳細に従い、本規約の発効と同時に両当事者間で適切に締結されたものとみなされます。

A) EUデータ移転条項

1. 第17条(準拠法)のオプション1が適用され、EU諸条項はルクセンブルク法に準拠すること、
2. 第18条(裁判地および管轄の選択)に従って、EU諸条項に起因する紛争は、ルクセンブルクの裁判所で解決すること、および
3. 両当事者は、EUデータ移転条項付属書に基づき要求される詳細が、別紙1に記載の通りであることに同意すること。

B) 英国データ移転条項

1. 条項II(h)(iii)が組み込まれ、PayPalによる本規約の署名がデータ輸入者としてPayPalに求められるイニシャルとみなされること、および
2. 両当事者は、適用可能な範囲において、UKデータ移転条項の別紙Bに基づき要求される詳細が付属書1に記載の通りであることに同意すること。

別紙1

EUデータ移転条項付属書および英国データ移転条項別紙B

A. EUデータ移転条項および英国データ移転条項に基づき、必要な範囲で以下が適用されます。

別紙1.A. 当事者リスト

データ輸出者

- 氏名および所在地: データ輸出者は売り手であり、所在地は本規約に記載の通り
- 担当者の氏名、役職、連絡先の詳細: 本規約に記載の通り
- 標準契約条項に基づき移転されたデータに関連するアクティビティ: 本規約に規定の通り
- 署名および日付: 本付帯条項の「国境を越えたデータ移転」のセクションを参照のこと
- 役割(管理者/処理者): 管理者

データ輸入者

- 氏名および所在地: データ輸入者は、本規約に従ってサービスを提供するPayPalのグループ会社であり、所在地は本規約に記載の通り
- 担当者の氏名、役職、連絡先の詳細: 本規約に記載の通り
- 標準契約条項に基づき移転されたデータに関連するアクティビティ: 本規約に規定の通り。署名および日付: 本付帯条項の「国境を越えたデータ移転」のセクションを参照のこと
- 役割(管理者/処理者): 管理者

別紙1.B. 移転の説明

データ対象者

移転される個人データは、以下のデータ対象者に関連するものです。

- データ輸出者およびその顧客、従業員、その他のビジネス関係者

移転される個人データのカテゴリ

移転される個人データには、以下のデータカテゴリが含まれる場合があります。

- 顧客の氏名、請求金額、日時、銀行口座の詳細、支払いカードの詳細情報、CVCコード、郵便番号、国名コード、住所、メールアドレス、ファックス、電話、ウェブサイト、有効期限情報、配送の詳細、税務申告の状況、顧客固有の識別子、IPアドレス、場所、および本規約の下でPayPalが受領したその他のデータ

機密情報(該当する場合)および適用の制限または保護措置

移転される個人データは、以下の機密情報カテゴリに関するものです。

- マーチャントが当該データを保存するようサービスを設定しない限り、適用されません。

制限と保護措置を適用します。

- マーチャントが当該データを保存するようサービスを設定しない限り、適用されません。

データ処理の性質

- 本規約に定めるものとします。

移転の目的

移転は以下の目的のために行われます。

- 本規約に従って、データ輸入者がデータ輸出者に対して提供するサービスの遂行
- データ輸入者、データ輸出者またはその顧客に影響を与える、または与える可能性のある不正行為およびリスクの特定
- データ輸入者に適用されるべき法律の遵守
- データ保護に関する付帯条項に規定の通り

個人データが保管される期間(不可能な場合は期間決定のために使用される基準)

データ輸入者は、収集目的に照らして必要な期間に限り、個人データを保管します(上記の目的をご覧ください)。個人データの適切な保管期間を決定するためデータ輸入者は、個人データの量、性質、機密性、個人データを承認なく使用または開示することによる潜在的なリスク、個人データの処理目的、その目的がその他の手段を通じて達成できるか否か、および適用される法律、規制、税務、会計、その他の要件を考慮します。

(下請け)処理者に移転する場合は処理の対象、性質および期間も指定

データ輸入者は、データ輸入者の指示の下でその代理でサービスを実行し機能する第三者のサービス提供者と個人データを共有することがあります。これらの第三者のサービス提供者は、例えば、顧客の本人確認、取引処理、カスタマーサポートなど、本契約に基づいて提供されるサービスの要素を提供し、データ保管など、本規約に基づいて提供されるサービスを支援するサービスをデータ輸入者に

提供することがあります。第三者のサービス提供者が処理を行う期間を決定する際、データ輸入者は、別紙1.Bに規定する基準を適用します。

別紙1.C. 監督当局

EUデータ移転条項の第13条(a)に従い、監督当局は、データ移転に関しデータ輸出者が規制(EU)2016/679に準拠することを保証する責任を負う管轄の監督当局として機能するものとしします。

別紙II. データセキュリティを確保するための技術的および組織的な対策

1. データ移転時のデータの仮名化、暗号化、および保護

PayPalのポリシーでは、本原則の遵守および個人データの開示リスク回避を保証するため、技術的コントロールを義務付けています。PayPalでは、全個人データの移転時および保管時に暗号化を採用する他、必要に応じて個人データ保護のため、トークン化などの業界標準の仮名化技術を採用しています。PayPalは、社内および第三者とのデータ移転に関しデータ保護のための主要な義務およびプロセスを定めた包括的なポリシーを有します。

2. 変更管理および事業継続性

PayPalの堅牢な変更管理プロセスは、変更が適切に計画、承認、実行および確認されることを保証することにより、データおよびシステムの継続的な可用性および回復力を全ステージを通じて保護します。会社の事業継続管理プロセスでは、主要関係者の利益を守るため効率的に対応できる能力を備えた組織回復力を構築するための枠組みを提供します。

3. 災害復旧

PayPalの堅牢な災害復旧プログラムは、重要なビジネスプロセスおよび顧客との取引を支援するITシステムに重点を置いており、重大な障害が発生した際に情報またはテクノロジーシステムを復旧させるためのプロセスがあります。PayPalのテクノロジーインフラは、プライマリおよびセカンダリの複数の安全なデータセンターに分散されており、それぞれがネットワークおよびセキュリティインフラ、専用アプリケーションおよびデータベースサーバー、ストレージを備えています。

4. 技術的および組織的な対策の有効性の定期的なテスト、審査および評価

PayPalは、技術的および組織的な対策の有効性を審査および評価するため、会社のテストプログラムを定期的に計画、実行し、結果を報告しています。本プログラムは、関係者と協力してテスト、報告および是正措置に必要な情報を取得・評価する、弊社企業リスクおよびコンプライアンスチームが管理しています。

5. ユーザーの識別および認証

PayPalのアクセス管理プロセスでは、ユーザーが対象アプリにアクセスする前に、ユーザーの識別および認証を行うため、固有のアカウントIDおよびパスワードを使用して企業ネットワークにログインする必要があります。パスワードの構成、長さ、変更、再利用、およびロックに関する自動ポリシーが適用されます。役割ベースによるアクセスおよび認証は四半期ごとに更新されます。これは権限を最小限に抑えることを原則とし対象となる全システムに実行されます。

6. 個人データ処理地点の物理的なセキュリティ

PayPalのグローバル安全セキュリティポリシーおよびプロセスでは、適用されるべき法律、規制、およびパートナーの要件に基づき、物理的な安全性を含む、安全・セキュリティプロセスの促進に必要な要件を定めています。メールルーム、機器保管庫、発送・受取エリア、コンピュータ/サーバールーム、通信保管庫、機密書類/情報保管エリアなど、特に機密性の高いエリアを建造する際は、会社の情報セキュリティ処理基準に従って、セキュリティシステムおよび保護措置に重点が置かれます。

7. イベントの記録および設定

PayPalでは、イベントの記録および監視の種類および属性を概説し定義しています。会社は、複数種類の記録を収集し、集中型セキュリティ監視システムに集約します。システムからログの記録を確実に収集し集中型セキュリティ監視システムに転送されるよう、標準的な設定管理統制が実施されています。また、PayPalのポリシーと支援プロセスでは、システム構成および強化ベースラインを全システムで実施することが定められています。

8. ITガバナンスおよび管理、プロセスおよび製品の証明と保証

PayPalは、全社的に強固なセキュリティ理念の推進を行っています。弊社の情報セキュリティ最高責任者は、グローバル全体で情報セキュリティの監督をしています。企業リスクおよびコンプライアンス管理プログラムの一環として、弊社の

テクノロジーの監視および情報セキュリティプログラムは、テクノロジーおよび情報セキュリティリスクの管理、および情報セキュリティの脅威に関わる特定、保護、検出、対応および回復のため、会社を支援するよう策定されています。PayPalは、以下の各種企業プログラムを通じてプロセスおよび製品の認証および保証を行っています。(i)ISO 27001、Payment Card Industry(PCI)の適用基準(DSS、PIN、P2PEなど)および米国公認会計士協会(AICPA)のSOC-1およびSOC-2(これだけに限定されません)に対するPayPalの業界標準義務に関する監査および評価、(ii)製品ソリューションの開発およびリリースに関連するリスクの測定、管理、および監視に対する早期の関与および標準的アプローチを保証するリスク管理識別プロセス(RCIP)、(iii)製品およびソフトウェア開発プロセスの初期段階に組み込まれたプライバシー影響評価、ならびに(iv)第三者との契約期間を通してリスクを継続的に管理することを保証する包括的な第三者管理プログラム。

9. データの最小化

弊社のポリシーでは、技術的コントロールを通じて、収集および生成されるデータ要素が適切かつ関連性があり、処理の目的に必要なものだけに限定されることを要求しています。PayPalのプライバシー影響評価プロセスは、これらポリシーへの準拠を保証します。

10. データの品質および保管

PayPalのアクセスおよび品質ポリシーは、個々のユーザーがシステムにアクセスし詳細情報(住所、連絡先の詳細など)を修正および変更できるようにすることによって、すべての個人データが正確、完全かつ最新であるようにします。データ主体から修正要求を受けた場合、修正の権利を行使できるサービスを提供します。弊社のデータガバナンスプログラムでは、データの品質、問題および修正を必要に応じて監視します。すべてのデータは、事業価値に応じて分類され、PayPalの法律、規制およびPayPal業務上の記録保管要件に基づいて保管期間が設定されなければなりません。保管期間が終了したデータおよび情報は、処分、削除または破棄されます。

11. 説明責任

PayPalは、一連の情報セキュリティ、テクノロジー、データガバナンス、第三者管理およびプライバシーに関連するポリシーおよび原則を策定しました。これらは業界標準に準拠したものであり、組織全体で関係者の協力とパートナーシップを得て当該ポリシーおよびコントロールの認識と遵守を高め、上層部から下層部まで組織全体の参加と説明責任を確保するためのものです。各プログラムでは、職域を超えたデータ関連の決定、プロセスおよびコントロールに関する説明責任

を定義します。PayPalは、データ管理者としてプライバシーに関する法律、規制、ポリシーおよび手順を全社的に遵守するため、プライバシープログラムポリシーと、何層もの組織的および技術的コントロールの基礎構造を設置することにより、GDPRおよびその他の適用されるデータ保護法における説明責任を伴う関連条項を遵守する責任を果たし、この遵守を証明しています。これには、次の方法によりデータ保護法の遵守を証明することが含まれます。1)コンプライアンス重視の企業文化、2)経営委員会、監督の役割、プライバシーに関する報告などの企業リスクおよび遵守のためのガバナンス構造、3)ビジネスプロセスおよびコントロールの確立、文書化、維持など、プライバシープログラムの遵守について事業部門の説明責任、4)企業コンプライアンス組織内のグローバルプライバシー部門による、事業におけるプライバシープログラムの遵守の監督、および事業部門が活用するポリシー、標準、手順およびツールの定義、5)プライバシーの認識と理解を促進するグローバルプライバシー部門による企業内での連絡、6)プライバシーへの影響評価、プライバシーの監視およびテスト、プライバシー問題の管理、プライバシーのトレーニング、年間プライバシー計画など一貫したプロセスの使用を確実にするための企業リスクおよびコンプライアンス管理の枠組み、ならびに7)プライバシープログラムを監督する経営委員会への報告および分析。

12. データ主体の権利

PayPalは、アクセス、修正および消去など、データ主体の権利が確実に履行されるためのプログラムを有します。PayPalがデータを保管する法的義務、規制上の義務、またはその他の正当な事業上の理由がない限り、データ消去の要求は履行されます。PayPalのポリシーは、お客様の利用を通して消去が確実に実行されることを保証します。

13. 処理者

PayPalは、包括的な第三者管理プログラムを有し、第三者との契約期間を通してリスクを継続的に管理することを保証します。弊社は、契約において処理者および下請け処理者に対し、処理工程全体で包括的なデータセキュリティおよびプライバシー基準を導入することを義務付けています。すべての下請け処理者は、契約前に事前承認を得る必要があります。

B. 以下は英国データ移転条項にのみ適用されます。

受取人

移転された個人データは、以下の受取人にのみ開示することができます。

- 本規約に基づく輸入者のサービスプロバイダ、関連会社、およびサービスを遂行する人物

データ輸出者のデータ保護登録情報(該当する場合)

適用されません。

有用な付属情報(保管期限などの関連情報)

本契約および上記別紙1に記載の通り。